Discipline: Computer Information Systems

Originator: James Cregg

RIVERSIDE COMMUNITY COLLEGE DISTRICT
INTEGRATED COURSE OUTLINE OF RECORD

COMPUTER INFORMATION SYSTEMS 27

CIS-27 : Information and Network Security

College: RIV
Lecture Hours: 54.000
Units: 3.00
Letter Grade

Course Description

Prerequisite: None

Advisory: CIS-1A or CIS-23

Course Credit Recommendation: Degree Credit

An introduction to the fundamental principles and topics of Information Technology Security and Risk Management at the organizational level. It addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational Cybersecurity and Risk Management. Preparation for the CompTIA Security+ certification exams. 54 hours lecture.

Short Description for Class Schedule

Information security, addresses hardware, software, processes, communications, applications, and policies and procedures with respect to organizational Cybersecurity and Risk Management.

Entrance Skills:

Before entering the course, students should be able to demonstrate the following skills:

1. **Demonstrate the principles of security system development methodology.**
   - **CIS-23** - Demonstrate the principles of configuration, memory management and diagnostic utilities to optimize computer performance.
2. **Apply the fundamental concepts of information security to network management and technology security.**
3. **Identify the functions and applications that apply to security systems development programs.**
   - **CIS-23** - Identify the functions of computer microprocessors, memory and peripheral components.

Student Learning Outcomes:

Upon successful completion of the course, students should be able to demonstrate the following skills:

1. **Describe the fundamental principles of information systems security.**
   - **Critical Thinking:** Students will be able to demonstrate higher-order thinking skills about issues, problems, and explanations for which multiple solutions are possible. Students will be able to explore problems and, where possible, solve them. Students will be able to develop, test, and evaluate rival hypotheses. Students will be able to construct sound arguments and evaluate the arguments of others.
   - **Information Competency & Technology Literacy:** Students will be able to use technology to locate, organize, and evaluate information. They will be able to locate relevant information, judge the reliability of sources, and evaluate the evidence contained in those sources as they construct arguments, make decisions, and solve problems.
2. **Define the concept of threat, evaluation of assets, information assets, physical, operational, and information security and how they are related.**
   - **Information Competency & Technology Literacy:** Students will be able to use technology to locate, organize, and evaluate information. They will be able to locate relevant information, judge the reliability of sources, and evaluate the evidence contained in those sources as they construct arguments, make decisions, and solve problems.
   - **Critical Thinking:** Students will be able to demonstrate higher-order thinking skills about issues, problems, and explanations for which multiple solutions are possible. Students will be able to explore problems and, where possible, solve them. Students will be able to develop, test, and evaluate rival hypotheses. Students will be able to construct sound arguments and evaluate the arguments of others.

3. **Evaluate the need for the careful design of a secure organizational information infrastructure.**
    - **Information Competency & Technology Literacy:** Students will be able to use technology to locate, organize, and evaluate information. They will be able to locate relevant information, judge the reliability of sources, and evaluate the evidence contained in those sources as they construct arguments, make decisions, and solve problems.
4. **Perform risk analysis and risk management.**
    - **Critical Thinking:** Students will be able to demonstrate higher-order thinking skills about issues, problems, and explanations for which multiple solutions are possible. Students will be able to explore problems and, where possible, solve them. Students will be able to develop, test, and evaluate rival hypotheses. Students will be able to construct sound arguments and evaluate the arguments of others.
    - **Communication Skills:** Students will be able to communicate effectively in diverse situations. They will be able to create, express, and interpret meaning in oral, visual, and written forms. They will also be able to demonstrate quantitative literacy and the ability to use graphical, symbolic, and numerical methods to analyze, organize, and interpret data.
5. **Determine both technical and administrative mitigation approaches.**
    - **Critical Thinking:** Students will be able to demonstrate higher-order thinking skills about issues, problems, and explanations for which multiple solutions are possible. Students will be able to explore problems and, where possible, solve them. Students will be able to develop, test, and evaluate rival hypotheses. Students will be able to construct sound arguments and evaluate the arguments of others.
    - **Communication Skills:** Students will be able to communicate effectively in diverse situations. They will be able to create, express, and interpret meaning in oral, visual, and written forms. They will also be able to demonstrate quantitative literacy and the ability to use graphical, symbolic, and numerical methods to analyze, organize, and interpret data.
6. **List and define the major categories of scanning and analysis tools, and describe the specific tools used within each of these categories.**
    - **Critical Thinking:** Students will be able to demonstrate higher-order thinking skills about issues, problems, and explanations for which multiple solutions are possible. Students will be able to explore problems and, where possible, solve them. Students will be able to develop, test, and evaluate rival hypotheses. Students will be able to construct sound arguments and evaluate the arguments of others.
    - **Information Competency & Technology Literacy:** Students will be able to use technology to locate, organize, and evaluate information. They will be able to locate relevant information, judge the reliability of sources, and evaluate the evidence contained in those sources as they construct arguments, make decisions, and solve problems.
7. **Describe the technology that enables the use of Virtual Private Networks and identify the various approaches to remote access.**
    - **Critical Thinking:** Students will be able to demonstrate higher-order thinking skills about issues, problems, and explanations for which multiple solutions are possible. Students will be able to explore problems and, where possible, solve them. Students will be able to develop, test, and evaluate rival hypotheses. Students will be able to construct sound arguments and evaluate the arguments of others.

General Education Outcomes:

- **District General Education -** A2 Language and Rationality - Communication & Analytical Thinking
- **UC/CSU Transfer Course -** Yes

Course Content:

1. Procedures and security maintenance.
2. Monitoring the external and internal security environment.
3. Major protocols used for secure communications and understand the nature and execution of the dominant method of attack.
    a. TCP/IP Transmission Control Protocol/Internet Protocol
    b. SNTP Simple Mail Transfer protocol
    c. POP3 Post Office Protocol
    d. HTTP Hypertext Transfer Protocol
4. Isolation of the virtual environment.
5. Setting up a home office security system.
    a. Using a wireless router for home office security.
    b. Wireless encryption WPA2.
6. Approaches to remote and VPN access protection.
7. Malware and social engineering attacks.

8. Application and network attacks.
9. Vulnerability Assessment and Mitigating Attacks.
10. Host, application, and data security.
11. Network and wireless security.
12. Administering a secure network.
13. Access control fundamentals.
14. Authentication and account management.
15. Basic and advanced cryptography.
16. Business continuity and risk mitigation.
17. Understanding the need for security.
18. Understanding the legal, ethical, and professional issues in information security.
19. Firewalls and virtual Private Network (VPN), firewall rules and protecting remote connections.
20. Technologies used in firewall security and communication tools to secure local area networks.

Methods of Instruction:

Methods of instruction used to achieve student learning outcomes may include, but are not limited to, the following activities:

- Present lectures and text descriptions to define the functions of a Certified Information Systems Security Professional.
- Develop and assign class exercises such as drills and practice quizzes to define terms that relate to information security.
- Create and have students take part in cooperative learning tasks such as a small group or paired role play to name and apply effective communication tools and techniques.
- Develop and assign activities such as web quests, router setups, and presentations to assess the categories of skills and work habits.
- Develop and assign lab activities that are directed toward professional certification, that need mastery of Access Controls, Cryptography, Risk, and Security operations.
- Develop and assign tasks/activities such as web quests and online paper submissions to design an efficient network security policy.
- Develop lab assignments and tasks/activities to test security needed for a virtual Private Networks.
- Develop and assign activities such as to list 5 strategies to organize and manage home/security and office/security duties.
- Develop labs that deliver fundamental information security principles packed with real-world applications.

Methods of Evaluation:

Students will be evaluated for progress in and/or mastery of student learning outcomes using methods of evaluation which may include, but are not limited to, the following activities:

- Evaluation will include hands-on projects and a combination of examinations, presentations, discussions, or problem-solving assignments.
- Written/online journal or written online summaries designed to describe the functions and purposes of network security.
- Quizzes/examinations designed to define terms that relate to comprehensive security programs.
- Individual, small group, or paired presentations designed to find and apply effective communication tools and techniques.
- Written reports designed to assess the categories of skills and filtering technology needed for a secure environment.
- Written reports to show the ability to design an efficient information security policy.
- Individual security projects designed to find types of network security that lend themselves to application protocol verification and relate them to their areas of interest.
- Individual or class projects designed to test security technology and software security needed for network control.
- Written reports designed to find and list ways to manage and organize network/security and home/office security.
- Final written projects/exam report which summarizes, synthesizes, and evaluates learning experiences and reflects how the course might influence student's master security plan.

Sample Assignments:

Outside-of-Class Reading Assignments

- Textbook reading and/or other resource reading that cover the functions and purposes of information security and telecommuting or virtual environments, and describe an ergonomic and efficient network security.

Outside-of-Class Writing Assignments

- Develop online/distance learning tasks/activities such as web quests, router setups, and online presentations to assess the categories of skills and work habits of a secure work environment. Develop online/distance learning tasks/activities such as web quests, website reviews, and discussion posting to show types of employment that lend themselves to security work and relate them to their areas of information security. Develop and assign online/distance learning tasks/activities such as web quests and online paper submissions to design an ergonomic and efficient network security.

Other Outside-of-Class Assignments

- Online activities such as web quests in order to identify and list 5 strategies to organize and manage home/security and office/security duties.

Course Materials:

All materials used in this course will be periodically reviewed to ensure that they are appropriate for college level instruction. Possible texts include the following:

Ciampa, Mark. *Security + Guide to Network Security Fundamentals.* 4nd Cengage Learning, 2012.
Kim, David, & Solomon, Michael. *Fundamentals of Information Systems Security.* 2nd Jones & Bartlett Learning, 2015.
Smith, Richard E. . *Elementary information Security.* 2nd Jones & Barlett Learning, 2015.
Whitman, Michael. *Principles of Information Security* . 5th Edition Cengage Learning, 2015.

Codes/Dates:

CB05 MOV Transfer Status: N/A (not in college inventory) (D)
CB05 NOR Transfer Status: N/A (not in college inventory) (D)
CB05 RIV Transfer Status: Transfers to CSU Only (B)

Board of Trustees Approval Date: 12/08/2015
COR Rev Date: 12/08/2015